

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

MARK KRENZER, individually and
on behalf of all others similarly
situated,

v.
Plaintiff,

USA WASTE-MANAGEMENT
RESOURCES, LLC,

Defendant.

Case No. 1-21-cv-6902

CLASS ACTION COMPLAINT
JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Mark Krenzer (“Plaintiff”), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to himself and on information and belief as to all other matters, by and through undersigned counsel, hereby files this Class Action Complaint against Defendant USA Waste-Management Resources, LLC (“Defendant,” “Waste Management,” or the “Company”). “Waste Management” also includes the Company’s affiliated entities.

I. NATURE OF THE ACTION

1. Hackers infiltrated and accessed the Company’s inadequately protected computer systems between January 21 and 23, 2021. During that time, the hackers stole the protected personal information of, among others Waste Management’s current and former employees, and their dependents, by hacking Waste Management’s computer systems and stealing their protected personal information. (“Private Information”). The Private Information that was stolen reportedly included current and former employees’ names, Social Security numbers or National IDs, health insurance policy information, dates of birth, driver’s license numbers, bank account numbers, debit and credit card numbers, as well as current and former employees’ (and their dependents’) medical

history and treatment information, health insurance information, passport numbers and usernames, email addresses, and passwords for financial electronic accounts (the “Data Breach”).¹

2. According to Waste Management’s notice to employees affected by the Data Breach, Waste Management reportedly discovered the Data Breach on January 21, 2021, but failed to timely notify affected individuals of the breach until late May and early June 2021 – more than four (4) months later.

3. On or about May 28, 2021, Waste Management began mailing breach notifications to affected current and former employees. According to Waste Management’s “Notice of Data Breach” sent to affected individuals, the Company discovered suspicious activity in its computer network environment on January 21, 2021. Thereafter, an investigation was commenced, and with the assistance of third-party forensic specialists, they sought to determine the nature and scope of the breach and contacted the FBI. Waste Management’s investigation determined the company suffered a cyberattack that allowed “an unauthorized actor” to access its computer network system between January 21 and 23, 2021 and steal certain files. On May 4, 2021, Waste Management determined that the accessed files “contained sensitive information” of current and former Waste Management employees, including Plaintiff Krenzer. Specifically, Waste Management’s investigation found that personal information on its current and former employees was in the hacked network system, including names, Social Security numbers, National IDs, health insurance policy information, dates of birth, and driver’s license numbers.

4. On information and belief, Plaintiff’s and Class members’ Private Information was stolen in the cyberattack. Plaintiff’s and Class members’ Private Information will now be used for criminal purposes, such as fraudulent text messaging schemes, email scams, identity theft and

¹*PHI of Employees Compromised in Cyberattack on Waste Management Firm*, <https://www.hipaajournal.com/phi-of-employees-compromised-in-cyberattack-on-waste-management-firm/> (last accessed on August 16, 2021); *Data Breach at US Waste Management Firm Exposes Employees’ Healthcare Details*, <https://portswigger.net/daily-swig/data-breach-at-us-waste-management-firm-exposes-employees-healthcare-details> (last accessed on August 16, 2021).

fraudulent purchases – including phishing, which is a criminal attack performed by cybercriminals to obtain sensitive information such as online passwords, by impersonating a reliable entity in a digital text or email communication – and sold by the actors responsible for the Data Breach to other criminals on the dark web.

5. Defendant's conduct – failing to take adequate and reasonable measures to ensure that its employee data was protected, failing to take adequate steps to prevent and stop the breach, failing to take adequate measures to detect the breach, failing to provide timely notice of the Data Breach so that more than four (4) months had passed before providing its current and former employees with notice of the breach, and enabling the actors to execute the Data Breach and steal Plaintiff's and Class members' Private Information – has caused substantial harm and injuries to its own employees and former employees.

6. Defendant Waste Management's material failures put Plaintiff's and Class members' Private Information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiff and Class members associated with time and money spent as a result of taking time and incurring costs to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach.

7. As a result of the Data Breach, Plaintiff and Class members have already suffered damages. For example, now that their Personal Information has been released into the criminal cyber domains including the dark web, Plaintiff and Class members are at imminent and impending risk of identity theft. This risk will continue for the rest of their lives, as Plaintiff and Class members are now forced to deal with the danger of identity thieves possessing and using their Personal Information. Additionally, Plaintiff and Class members have already lost time and money responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

8. Plaintiff brings this action individually and on behalf of the Class and seeks actual damages, statutory damages, punitive damages, and restitution, with attorney fees, costs, and expenses for, among other causes of action, negligence, breach of implied contract, breach of confidence, violation of New York GBL § 349, violation of New York Labor Law § 203-d, and unjust enrichment. Plaintiff also seeks declaratory and injunctive relief, including significant improvements to Defendant's data security systems and protocols, future annual audits, Defendant-funded long-term credit monitoring services, and other remedies as the Court deems necessary and proper.

II. JURISDICTION AND VENUE

9. This Court has diversity jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 class members, the amount in controversy exceeds \$5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

10. This Court has personal jurisdiction over Defendant Waste Management because it is a New York limited liability company with its registered address in New York.

11. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant conducts substantial business in this District, a part of the events giving rise to the claims set forth herein derived from activities within this District, and Defendant has caused harm to Class members residing in this District.

III. PARTIES

Plaintiff

12. Plaintiff Mark Krenzer is a citizen of the State of Texas. He received notice from Waste Management on or about June 4, 2021, informing him of the Data Breach.²

² Plaintiff Krenzer's data breach notification letter from Waste Management is attached hereto as Exhibit "A".

13. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class members; (ii) warn Plaintiff and Class members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates state statutes.

14. Plaintiff and Class members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their Private Information, which may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

15. Defendant Waste Management obtained and continues to maintain Plaintiff Krenzer's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Krenzer would not have entrusted his Private Information to Defendant had he known that Waste Management would fail to maintain adequate data security. Plaintiff Krenzer's Private Information was compromised and disclosed as a result of the Data Breach.

16. As a result of the Data Breach, Plaintiff Krenzer anticipates spending considerable time on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Krenzer will continue to be at increased risk of identity theft and fraud

for years to come.

17. Like Plaintiff Krenzer, the other Class members have a continuing interest in ensuring that their Private Information is protected and safeguarded from future breaches.

18. The injuries suffered by Plaintiff and Class members as a direct result of the Data Breach include one or more of the following:

- a. unauthorized use of their Private Information;
- b. theft of their Private Information;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;
- d. damages arising from the inability to use their Private Information;
- e. Time spent and costs associated with the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including a material increase in correspondence from purported debt collectors and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;
- f. damages to and diminution in value of their Private Information entrusted to Defendant by virtue of their employment by Defendant; and
- g. the loss of Plaintiff's and Class members' privacy.

Defendant

19. Defendant USA Waste--Management Resources, LLC is a New York limited liability company organized under the laws of New York with its registered address located at 28 Liberty Street, New York, New York 10005. Upon information and belief, USA Waste-Management Resources, LLC's sole member is Defendant Waste Management, Inc. ("WMI").

WMI is incorporated in Delaware and headquartered at 800 Capital Street in Houston, Texas. USA Waste-Management Resources, LLC is a subsidiary of and controlled by Defendant WMI.

20. Waste Management describes itself as the leading provider of comprehensive waste management, offering a range of services such as garbage collection and disposal, recycling and dumpster rental.

21. Defendant Waste Management is a major player in the waste management and recycling industry and employs over 45,000 employees. As a condition to their employment, Defendant requires its employees to provide their highly sensitive personal information.

22. Defendant Waste Management operates at the expense of its employees; however, Waste Management betrayed the trust of its employees by putting their Private Information at risk of attack by cybercriminals. Waste Management's actions and/or inaction exposed its customers' Private Information, including highly sensitive Private Information, to cyberattack. Through this lawsuit, the numerous affected current and former employees who entrusted their Private Information to Waste Management have a voice in Plaintiff Krenzer.

IV. STATEMENT OF FACTS

The Data Breach

23. On or about January 21, and through January 23, 2021, Defendant Waste Management's computer systems were subject to a cyberattack through which unauthorized third-party cybercriminals gained access to Plaintiff's and Class members' Private Information, including current and former employees' names, Social Security numbers or National IDs, health insurance policy information, dates of birth, driver's license numbers, bank account numbers, debit and credit card numbers, as well as current and former employees' (and their dependents') medical history and treatment information, health insurance information, passport numbers and usernames, email addresses, and passwords for financial electronic accounts.

24. Defendant Waste Management, having discovered the breach in January 2021, did not publicly acknowledge the Data Breach until late May 2021, over four (4) months after the breach occurred.

25. On or about May 28, 2021—four months after first learning of the Data Breach—Defendant began sending out Notices of Data Breach to its current and former employees whose information was stolen in the Data Breach.

26. It is apparent from the various notices and sample notices of the Data Breach sent to Plaintiff, the Class, and state Attorneys General that the Personal Information contained within its computer systems was not adequately secured and protected.

27. Following discovery of the Data Breach, Defendant began to investigate and address the Data Breach. Based upon the investigation, the hackers were able to access certain computer systems containing the Personal Information at issue.

28. Upon information and belief, the unauthorized third-party cybercriminals gained access to the Personal Information with the intent of engaging in misuse of the Personal Information, including marketing and selling Plaintiff's and Class members' Personal Information on the dark web.

29. In spite of the severity of the Data Breach, Defendant has not adequately protected Plaintiff and the Class. For example, upon information and belief, in the Data Breach Notice, Defendant only provide twelve (12) months of identity theft and credit monitoring protection.

30. In effect, Defendant is shirking its responsibility for the harm and increased risk of harm it has caused Plaintiff and members of the Class, including the distress and financial burdens the Data Breach has placed upon the shoulders of the Data Breach victims.

31. To make matters worse, Defendant's hackers gained access to, and possession of, Plaintiff's and Class members' Personal Information. While many data breach events merely involve

the attacker gaining access to the computer or network without meaningful access to the victims' information, in this particular attack on Defendant's systems, hackers gained access to Plaintiff's and Class members' highly sensitive Personal Information, including social security numbers and bank account and other financial information, as well as health insurance policy information.

32. Defendant failed to adequately safeguard Plaintiff's and Class members' Personal Information, allowing cyber criminals to access this wealth of priceless information for four (4) months before warning the criminals' victims to be on the lookout, and now offer them almost no remedy or relief.

33. Defendant failed to employ adequate resources on cybersecurity security measures and protocols.

34. Plaintiff and Class members were required to provide their Personal Information to Defendant as a condition of their employment and with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

35. The stolen Personal Information at issue has great value to the cyber-attackers, due to the large number of individuals affected and the fact that financial and bank account information and Social Security numbers were part of the data that was compromised.

Plaintiff Krenzer's Experience

36. Plaintiff Krenzer worked in corporate offices for Defendant Waste Management as a Senior Financial Analyst from 2008 to 2014.

37. As a condition to employment, Plaintiff Krenzer provided his personal identifying information to Defendant Waste Management, including his name, address, telephone number, personal email address, Social Security number, and bank account information, among other information. Plaintiff Krenzer also provided personal and other identifying information to enroll in

health insurance and life insurance offered by Waste Management, and to enroll in the Company's 401(k) retirement plan.

38. Plaintiff Krenzer received the data breach notice from Defendant Waste Management on or after June 4, 2021.

39. As a result of the Data Breach notice, Plaintiff is spending many hours dealing with the consequences of the Data Breach, including monitoring his bank accounts, credit card accounts, credit reports, and health and medical insurance data, and evaluating freezing his credit with credit reporting agencies and credit protection services. Following the Data Breach, Plaintiff began receiving correspondence from potential criminals posing as Amazon.com and the Internal Revenue seeking to recover purported unpaid debts, which Plaintiff must also address as a further unwanted consequence of the Data Breach including spending time with respect to same.

40. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns for the loss of his privacy, which he would not have suffered had Defendant implemented the necessary and proper safeguards to protect its employees' Private Information from theft.

41. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Defendant's Data Security Safeguards Were Inadequate

42. Defendant is required to protect Plaintiff's and Class members' Personal Information, and further, to handle any breach of the same in accordance with applicable federal and state law.

43. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing,

safeguarding, deleting, and protecting the Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Personal Information of the Class.

44. Defendant owed a duty to Plaintiff and the Class to design, maintain, and test its computer systems and networks to ensure that the Personal Information in Defendant's possession was adequately secured and protected.

45. Defendant owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the Personal Information in its possession.

46. Defendant owed a duty to Plaintiff and the Class to implement processes that would detect a breach on their data security systems in a timely manner.

47. Defendant owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

48. Defendant owed a duty to Plaintiff and the Class to timely disclose if their computer systems and data security practices were inadequate to safeguard individuals' Personal Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal Information with Defendant.

49. Defendant owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

50. Defendant owed a duty of care to Plaintiff and the Class because they were foreseeable and probable victims of any inadequate data security practices.

51. Plaintiff and other Class members relied on Defendant to implement and maintain systems that kept their Private Information safe. Defendant had a duty to keep its employees' Private

Information safe, particularly given the highly sensitive nature of the information stored on Defendant's computer systems. Defendant failed to comply with this duty.

Cyber Criminals Will Use Plaintiff's and Class Members' Personal Information for Nefarious Purposes

52. Plaintiff and Class members highly sensitive Personal Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can be used in a variety of ways for criminals to exploit Plaintiff and the Class members and to profit off their misfortune and stolen information.

53. Every year, identity theft causes tens of billions of dollars of losses to victims in the United States.³ For example, with the Personal Information stolen in the Data Breach, including Social Security numbers and bank account information, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.⁴ These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class members.

54. Personal Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.

55. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.⁵

³ *Facts + Statistics: Identity Theft and Cybercrime*, Insurance Info. Inst., <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

⁴ See, e.g., Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

⁵ Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), <https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info>.

56. Hackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁶

57. For instance, with a stolen Social Security number, which is part of the Personal Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.⁷

58. If cyber criminals manage to access financial information, health insurance policy information, and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendant may expose the Plaintiff and Class members.

Damages Sustained by Plaintiff and Class Members

59. Plaintiff and the other members of the Class have suffered injury and damages, including, but not limited to one or more of the following:

- a. unauthorized use of their Private Information;
- b. damages arising from the inability to use their Private Information;
- c. monetary costs associated with their attempts to ameliorate, mitigate and deal with the actual and future consequences of the breach, including the freezing of their credit;
- d. time spent and monetary and other costs associated with the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate,

⁶ *Stolen Laptops Lead to Important HIPAA Settlements*, U.S. Dep’t of Health and Human Services (Apr. 22, 2014), available at <https://wayback.archiveit.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolenlaptops-lead-to-important-hipaa-settlements.html>.

⁷ See, e.g., Christine DiGangi, 5 Ways an Identity Thief Can Use Your Social Security Number, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiff and Class members could have been working and earning a living, therefore suffering further actual injury);

- e. the imminent and impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;
- f. damages to and diminution in value of their Private Information entrusted to Defendant for the sole purpose of purchasing products and services from websites operated by Defendant; and
- g. the loss of Plaintiff's and Class members' privacy.

V. CLASS ACTION ALLEGATIONS

60. Plaintiff brings this action on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a nationwide Class defined as:

All natural persons residing in the United States whose Private Information was compromised in the Data Breach that occurred in January 2021 (the "Nationwide Class" or "Class").

61. In addition, Plaintiff brings this action on behalf of himself and on behalf of a subclass defined as:

All current and former employees of Defendant Waste Management who are residents of the United States of America and whose Private Information was compromised in the Data Breach that occurred in January 2021 (the "Employee Subclass").

62. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

63. Certification of Plaintiff's claims for class-wide treatment is appropriate because

Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

64. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number in the tens of thousands.

65. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

- a. Whether Defendant failed to use reasonable care and reasonable methods to secure and safeguard Plaintiff's and Class members' Private Information;
- b. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and Class members' Private Information from unauthorized capture, dissemination, and misuse;
- c. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- d. Whether Defendant disclosed Plaintiff's and Class members' Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- e. Whether Defendant failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class members' Private Information;
- f. Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and Class members' Private Information; and

g. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

66. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and other Class members. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

67. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

68. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because his interests do not conflict with the interests of the other Class members he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

69. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23(b)(2).

70. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other

financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

71. Plaintiff, individually and on behalf of the Class, repeats and re-alleges the allegations contained in paragraphs 1 through 70 as though fully set forth herein.

72. By virtue of its express undertaking to protect class members' personal information and upon accepting and storing Plaintiff's and Class members' Private Information, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use reasonable methods to do so. Defendant knew that the Private Information was confidential and should be protected as private and confidential.

73. Defendant owed a duty of care not to subject Plaintiff's and Class members' Private Information to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

74. Defendant owed numerous duties to its current and former employees, Plaintiff and Class members, including the following:

- a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information;
- b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches on its own systems and those of its third parties.

75. Defendant failed to provide adequate supervision and oversight of the Private Information with which it was, and is, entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' Private Information, misuse the Private Information and intentionally disclose it to others without consent.

76. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information, the vulnerabilities of its data collection and/or storage systems, and the importance of adequate security.

77. Defendant knew, or should have known, that its data collection and/or storage systems and networks, including its third-party affiliates, did not adequately safeguard Plaintiff's and Class members' Private Information.

78. Defendant breached its duties to Plaintiff and Class members by failing to ensure that its agents and affiliates were providing fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

79. Because Defendant knew that a breach of its systems would damage an untold number of its customers, including Plaintiff and Class members, Defendant had a duty to adequately safeguard its data systems and the Private Information contained thereon.

80. Defendant had a special relationship with Plaintiff and Class members by virtue of the employment relationship. Plaintiff's and Class members' willingness to entrust Defendant with their Private Information was predicated on the understanding and conditional requirement that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and those of its affiliates, and the Private Information it stored on them, from attack.

81. Defendant also had independent duties under state and federal laws that required it to reasonably safeguard Plaintiff's and Class members' Private Information and promptly notify them about the Data Breach.

82. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and its failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendant's possession or within its control or in the possession of its agent.

83. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the Private Information to Plaintiff and the Class members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information. Defendant failed to do so, only disclosing the Data Breach four (4) months after it occurred.

84. Upon information and belief, Defendant improperly and inadequately safeguarded

Plaintiff's and Class members' Private Information in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendant's failure to take proper security measures to protect Plaintiff's and Class members' sensitive Private Information, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of the Private Information.

85. Upon information and belief, neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

86. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members have suffered and will suffer damages and injury, including but not limited to:

- a. unauthorized use of their Private Information;
- b. theft of their Private Information;
- c. monetary costs associated with the detection and prevention of spam telephone calls, identity theft and unauthorized use of their Private Information;
- d. damages arising from the inability to use their Private Information;
- e. time spent and monetary and other costs associated with the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach (which time spent on those activities Plaintiff and Class members could have been working and earning a living, therefore suffering further actual injury);
- f. the imminent and impending injury flowing from spam phone calls and identity theft attempts posed by their Private Information being placed in the hands of criminals;
- g. damages to and diminution in value of their Private Information entrusted to

Defendant for the sole purpose of purchasing products and services from website operated by Defendant; and

- h. the loss of Plaintiff's and Class members' privacy.

87. As a direct and proximate cause of Defendant's negligence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to anxiety, emotional distress, loss of privacy, and other economic and non- economic losses.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Employee Subclass)

88. Plaintiff, individually and on behalf of the Class, repeats and re-alleges the allegations contained in paragraphs 1 through 70 as though fully set forth herein.

89. Defendant required Plaintiff and the Class to provide their personal information, including employees' names, dates of birth, Social Security numbers, driver's license numbers or state ID numbers, financial account and/or routing numbers, health insurance information, taxpayer identification numbers, and credit card numbers and/or expiration dates, as a condition of their employment.

90. As a condition of their employment with Defendant, Plaintiff and the Class provided their personal and financial information. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

91. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

92. Defendant breached the implied contracts they made with Plaintiff and the Class by

failing to safeguard and protect their personal, health/medical, and financial information, and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the data breach.

93. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
Breach of Confidence
(On Behalf of Plaintiff and the Employee Subclass)

94. Plaintiff, individually and on behalf of the Employee Subclass, repeats and re-alleges the allegations contained in paragraphs 1 through 70 as though fully set forth herein.

95. At all times during Plaintiff's and the Employee Subclass' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and the Employee Subclass' Private Information that Plaintiff and the Employee Subclass—employed by Defendant—provided to Defendant.

96. As alleged herein and above, Defendant's relationship with Plaintiff and the Employee Subclass was governed by terms and expectations that Plaintiff's and the Employee Subclass' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

97. Plaintiff and the Employee Subclass employed by Defendant provided Plaintiff's and the Employee Subclass' Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

98. Plaintiff and the Employee Subclass employed by Defendant also provided Plaintiff's and the Employee Subclass' Private Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that Private Information from unauthorized disclosure.

99. Defendant voluntarily received in confidence Plaintiff's and the Employee Subclass' Private Information with the understanding that Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

100. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiff's and the Employee Subclass' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and the Employee Subclass' confidence, and without their express permission.

101. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Employee Subclass have suffered damages.

102. But for Defendant's disclosure of Plaintiff's and the Employee Subclass' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and the Employee Subclass' Private Information as well as the resulting damages.

103. The injury and harm Plaintiff and the Employee Subclass suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and the Employee

Subclass' Private Information. Defendant knew or should have known its methods of accepting and securing Plaintiff's and the Employee Subclass' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and the Employee Subclass' Private Information.

104. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and the Employee Subclass, Plaintiff and the Employee Subclass have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of current and former employees; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Employee Subclass.

105. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Employee Subclass have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT IV
Violation of N.Y. Gen. Bus. Law § 349

106. Plaintiff, individually and on behalf of the Nationwide Class, repeats and re-alleges the allegations contained in paragraphs 1 through 70 as though fully set forth herein.

107. New York General Business Law (“NYGBL”) § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

108. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a “business practice” within the meaning of the NYGBL § 349, and the deception occurred in part within New York State.

109. Defendant stored Plaintiff’s and the Nationwide Class members’ Private Information in Defendant’s electronic and consumer information databases. Defendant knew or should have known that it did not employ reasonable, industry standard, and appropriate security measures that complied “with federal regulations” and that would have kept Plaintiff’s and the Nationwide Class members’ Private Information secure and prevented the loss or misuse of Plaintiff’s and the Nationwide Class members’ Private Information. Defendant did not disclose to Plaintiff and the Nationwide Class members that its data systems were not secure.

110. Plaintiff and the Nationwide Class members never would have provided their sensitive and personal Private Information if they had been told or knew that Defendant failed to maintain sufficient security to keep such Private Information from being hacked and taken by others, and that Defendant failed to maintain the information in a properly encrypted form.

111. Defendant violated the NYGBL §349 by failing to properly represent, both by affirmative conduct and by omission, the safety of Defendant’s many systems and services, specifically the security thereof, and their ability to safely store Plaintiff’s and the Nationwide Class members’ Private Information.

112. Defendant also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or adequately follow industry standards for data security, and by failing to immediately notify Plaintiff and the Nationwide Class members of the Data Breach. If Defendant had complied with these legal requirements, Plaintiff and the other Nationwide Class members would not have suffered the extent of damages caused by the Data Breach.

113. Defendant's practices, acts, policies and course of conduct violate NYGBL § 349 in that:

- a. Defendant actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff and the Nationwide Class members at the time they provided such Private Information that Defendant did not have sufficient security or mechanisms to protect Private Information; and
- b. Defendant failed to give timely warnings and notices regarding the defects and problems with its system(s) of security that it maintained to protect Plaintiff's and the Nationwide Class members' Private Information.

114. Plaintiff and Nationwide Class members were entitled to assume, and did assume, Defendant would take appropriate measures to keep their Private Information safe. Defendant did not disclose at any time that Plaintiff's and the Nationwide Class members' Private Information was vulnerable to hackers because Defendant's data security measures were inadequate, and Defendant was the only one in possession of that material information, which it had a duty to disclose.

115. The aforementioned conduct constitutes an unconscionable commercial practice in that Defendant has, by the use of false statements and/or material omissions, failed to properly represent and/or concealed the defective security system it maintained and failed to reveal the Data Breach timely and adequately.

116. Such acts by Defendant are and which are and/or were likely to mislead a reasonable

person providing his or her Private Information to Defendant. Said acts and practices are material. The requests for and use of such Private Information in New York through such means occurring in New York were consumer-oriented acts and thereby fall under the New York consumer protection statute, NYGBL § 349.

117. Defendant's wrongful conduct caused Plaintiff and the Nationwide Class members to suffer a consumer-related injury by causing them to incur actual and future loss of time and expense to protect from misuse of the Private Information materials by third parties and placing Plaintiff and the Nationwide Class members at serious risk for monetary damages.

118. As a direct and proximate cause of Defendant's conduct, Plaintiff and Nationwide Class members suffered damages as alleged above.

119. In addition to or in lieu of actual damages, because of the injury, Plaintiff and the Nationwide Class members seek statutory damages for each injury and violation which has occurred.

COUNT V
Negligence *Per Se*
Violation of New York Labor Law § 203-d
(On Behalf of Plaintiff and the Employee Subclass)

120. Plaintiff, individually and on behalf of the Class, repeats and re-alleges the allegations contained in paragraphs 1 through 70 as though fully set forth herein.

121. Pursuant to New York Labor Law § 203-D, an employer shall not, unless otherwise required by law: (a) publicly post or display an employee's social security number; (b) visibly print a social security number on any identification badge or card, including any time card; (c) place a social security number in files with unrestricted access; or (d) communicate an employee's personal identifying information to the general public.

122. For purposes of New York Labor Law § 203-D, "personal identifying information" shall include an individual's social security number, home address or telephone number, personal electronic mail address, Internet identification name or password, parent's surname prior to

marriage, or drivers' license number.

123. It shall be presumptive evidence that a violation of New York Labor Law § 203-D was knowing if the employer has not put in place any policies or procedures to safeguard against such violation, including procedures to notify relevant employees of these provisions.

124. Defendant failed to provide reasonable security, safeguards, policies, and procedures, and protections to the personal data of Plaintiff and Employee Subclass members, instead permitting unauthorized third parties access to Plaintiffs' and Employee Subclass members' Private Information.

125. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and the Employee Subclass members' Private Information was disclosed to unauthorized third parties causing damage to Plaintiff and the Employee Subclass.

126. Accordingly, Plaintiff and the Employee Subclass seek relief under New York Labor Law § 203-d, including actual damages, statutory damages, injunctive relief, and/or attorneys' fees, expenses, and costs.

COUNT VI
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class)

127. Plaintiff, individually and on behalf of the Nationwide Class, repeats and re-alleges the allegations contained in paragraphs 1 through 70 as though fully set forth herein.

128. By engaging in the conduct described in this Complaint, Defendant has knowingly obtained benefits from Plaintiff and the Nationwide Class, namely their labor and the profits therefrom, and actual monies and other benefits under circumstances such that it would be inequitable and unjust for this Defendant to retain them.

129. By engaging in the acts and failures to act described in this Complaint, Defendant has been knowingly enriched by the savings in costs that should have been reasonably expended to

protect the Private Information of Plaintiff and the Nationwide Class. Defendant knew or should have known that theft of employee Private Information could happen, yet it failed to take reasonable steps to pay for the level of security required to have prevented the theft of its current and former employees' Private Information.

130. By engaging in the conduct described in this Complaint, Defendant has knowingly obtained benefits from Plaintiff and the Nationwide Class under circumstances such that it would be inequitable and unjust for Defendant to retain them.

131. Defendant will be unjustly enriched if it is permitted to retain the benefits derived from the theft of Plaintiff's and the Nationwide Class's Private Information.

132. Plaintiff and each member of the Nationwide Class are therefore entitled to an award of compensatory damages in an amount to be determined at trial, or the imposition of a constructive trust upon the monies derived by Defendant by means of the above-described actions.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in his and the Class's favor and against Defendant, as follows:

- A. Declaring that this action is a proper class action, certifying the Nationwide Class and Employee Subclass as requested herein, designating Plaintiff as Class Representative, and appointing Class Counsel as requested in Plaintiff's expected motion for class certification;
- B. Ordering Defendant to pay actual/statutory damages as appropriate to Plaintiff and the other members of the Class;

- C. Ordering Defendant to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;
- D. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiff and his counsel;
- E. Ordering Defendant to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;
- F. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and
- G. Ordering such other and further relief as may be just and proper.

Date: August 16, 2021.

Respectfully submitted,

/s/ Lori G. Feldman
Lori G. Feldman (LF-3478)
GEORGE GESTEN MCDONALD PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Phone: (917) 983-9321
Fax: (888) 421-4173
Email: LFeldman@4-Justice.com
E-Service: eService@4-Justice.com

David J. George*
Brittany L. Brown*
GEORGE GESTEN MCDONALD, PLLC
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
Phone: (561) 232-6002
Fax: (888) 421-4173
Email: DGeorge@4-Justice.com
BBrown@4-Justice.com
E-Service: eService@4-Justice.com

Attorneys for Plaintiff

**Pro hac vice forthcoming*